

iPhone Vulnerability Makes Messages Sent via iMessage Unsecured Using Apple's Default Settings

Users discovered Apple's iPhone contains a major vulnerability that makes private messages sent via iMessage unsafe if you use Apple's default settings.

Specifically, a flaw in the iCloud backup system could make your private messages accessible outside of the app.

Apple only encrypts users' messages on messaging apps like [iMessage](#) and WhatsApp but doesn't encrypt its backups on cloud servers making security that helps keep messaging apps safe. reduce.



A recent leak of FBI documents shows that US intelligence agencies regularly access personal data from nine different "encrypted" messaging services. And one of them is Apple's iMessage. Even, "if the target is using an iPhone and has iCloud backup enabled, the iCloud backups may contain message content data", the [FBI](#) can access some of the message content.

Fortunately, users can protect their chats from being eavesdropped by others by changing iCloud's default settings. Go to the Settings app > select Apple ID > iCloud > Tap the "iCloud Backup" option and turn it off.



With just a small change in settings, the iPhone's iMessage message security level makes a big difference: The left side is fully secure and the right side is completely unsecured .

You finished reading the article "**iPhone Vulnerability Makes Messages Sent via iMessage Unsecured Using Apple's Default Settings**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.